AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A tamper detection system for securing a protected integrated circuit from attack, the tamper detection system comprising:

a power source;

a trigger circuit including a plurality of resistors and a plurality of wire loops, the plurality of resistors including a first resistor, a second resistor and a third resistor, all of which being wired together in series and operatively connected to the power source, the plurality of wire loops including a first wire loop extending between the first resistor and the second resistor and a second wire loop extending between the second resistor and the third resistor, the first wire loop and the second wire loop being electrically isolated from each other but in physical proximity to each other so as to form a protective mesh that envelopes the protected integrated circuit; ~~and~~

a ground layer in physical proximity to the first wire loop or the second wire loop; and

a detection circuit being in operative communication with the trigger circuit and the protected integrated circuit, the detection circuit including a first transistor and a second transistor, the first transistor being operatively connected across the second resistor so that the first transistor is controlled by a bias voltage across the second resistor, the second transistor being operatively connected across the first transistor and ground so that the second transistor is activated by an output current received from the first transistor, the detection circuit monitoring a flow of current through the trigger circuit, wherein if the flow of current through the trigger circuit is altered because of an open condition in the first wire loop or the second wire loop or a short between the first wire loop and the second wire loop or a short from the first wire loop or the second wire loop to the ground layer, then the detection circuit outputs a predetermined signal at a designated node located between the power source and the second transistor.

2. Cancelled.

3. Cancelled.

4. (Currently Amended) The tamper detection system of claim 1 ~~3~~, wherein:

the detection circuit further includes a fourth ~~forth~~ resistor connected between the power source and the second transistor;

the first transistor is a PNP type having an emitter node, a base node and a collector node, the first transistor emitter node is connected between the first resistor and the second resistor, the first transistor base node is connected between the second resistor and the third resistor;

the second transistor is a NPN type having an emitter node, a base node and a collector node, the second transistor base node is connected to the first transistor collector node, the second transistor emitter node is connected to ground, the second transistor collector node is connected to the fourth ~~forth~~ resistor; and

the designated node is between the fourth ~~forth~~ resistor and the second transistor collector node.

5. (Currently Amended) The tamper detection system of claim 4, wherein~~:~~ the predetermined signal is a high voltage condition substantially equal to the power source.

6. (Currently Amended) A ~~The~~ tamper detection system ~~of claim 1, wherein:~~ for securing a protected integrated circuit from attack, the tamper detection system comprising:

a power source;

a trigger circuit including a plurality of resistors and a plurality of wire loops, the plurality of resistors including a first resistor, a second resistor and a third resistor, all of which being wired together in series and operatively connected to the power

source, the plurality of wire loops including a first wire loop extending between the first resistor and the second resistor and a second wire loop extending between the second resistor and the third resistor, the first wire loop and the second wire loop being electrically isolated from each other but in physical proximity to each other so as to form a protective mesh that envelopes the protected integrated circuit; and

a detection circuit being in operative communication with the trigger circuit and the protected integrated circuit, the detection circuit including ~~includes~~ a first transistor and a second transistor, the first transistor being~~is~~ operatively connected across the second resistor so that the first transistor is controlled by ~~allowed to develop~~ a bias voltage across ~~cross~~ the second resistor, the second transistor being ~~is~~ operatively connected across the first transistor and ground so that the second transistor is activated by an output current received from the first transistor, the detection circuit monitoring a flow of current through the trigger circuit, wherein if the flow of current through the trigger circuit is altered because of an open condition in the first wire loop or the second wire loop or a short between the first wire loop and the second wire loop then the detection circuit outputs a predetermined signal at ~~and the~~ a designated node ~~is~~ located between the power source and the second transistor.

7. (Currently Amended) The tamper detection system of claim 6, wherein:

the detection circuit further includes a fourth ~~forth~~ resistor connected between the power source and the second transistor;

the first transistor is a PNP type having an emitter node, a base node and a collector node, the first transistor emitter node is connected between the first resistor and the second resistor, the first transistor base node is connected between the second resistor and the third resistor;

the second transistor is a NPN type having an emitter node, a base node and a collector node, the second transistor base node is connected to the first transistor

collector node, the second transistor emitter node is connected to ground, the second transistor collector node is connected to the fourth ~~forth~~ resistor; and

the designated node is between the fourth ~~forth~~ resistor and the second transistor collector node.

8. (Currently Amended) The tamper detection system of claim 7, wherein: the predetermined signal is a high voltage condition substantially equal to the power source.

9. (Currently Amended) A method of producing a tamper detection system for securing a protected integrated circuit from attack, the method comprising ~~the step(s) of~~:

providing a power source;

providing a trigger circuit including a plurality of resistors and a plurality of wire loops, the plurality of resistors including a first resistor, a second resistor and a third resistor, all of which being wired together in series and operatively connected to the power source, the plurality of wire loops including a first wire loop extending between the first resistor and the second resistor and a second wire loop extending between the second resistor and the third resistor;

keeping the first wire loop and the second wire loop electrically isolated from each other;

placing the first wire loop and the second wire loop in physical proximity to each other so as to form a protective mesh that envelopes the protected integrated circuit; ~~and~~

providing a ground layer in physical proximity to the first wire loop or the second wire loop;

providing a detection circuit in operative communication with the trigger circuit and the protected integrated circuit, the detection circuit including a first transistor

and a second transistor, the first transistor being operatively connected across the second resistor so that the first transistor is controlled by a bias voltage across the second resistor, the second transistor being operatively connected across the first transistor and ground so that the second transistor is activated by an output current received from the first transistor, the detection circuit monitoring a flow of current through the trigger circuit, wherein if the flow of current through the trigger circuit is altered because of an open condition in the first wire loop or the second wire loop or a short between the first wire loop and the second wire loop or a short between the first wire loop or second wire loop and the ground layer, then the detection circuit outputs a predetermined signal at a designated node located between the power source and the second transistor.

10. Cancelled.

11. Cancelled.

12. (Currently Amended) The method of claim 9 ~~11~~, wherein:

the detection circuit further includes a fourth ~~forth~~ resistor connected between the power source and the second transistor;

the first transistor is a PNP type having an emitter node, a base node and a collector node, the first transistor emitter node is connected between the first resistor and the second resistor, the first transistor bias node is connected between the second resistor and the third resistor;

the second transistor is a NPN type having an emitter node, a base node and a collector node, the second transistor base node is connected to the first transistor collector node, the second transistor emitter node is connected to ground, the second transistor collector node is connected to the fourth ~~forth~~ resistor; and

the designated node is between the fourth ~~forth~~ resistor and the second transistor collector node.

13. (Currently Amended) The method of claim 12, wherein: the predetermined signal is a high voltage condition substantially equal to the power source.

14. (Currently Amended) A ~~The~~ method ~~of claim 9, wherein:~~ of producing a tamper detection system for securing a protected integrated circuit from attack, the method comprising:

providing a power source;

providing a trigger circuit including a plurality of resistors and a plurality of wire loops, the plurality of resistors including a first resistor, a second resistor and a third resistor, all of which being wired together in series and operatively connected to the power source, the plurality of wire loops including a first wire loop extending between the first resistor and the second resistor and a second wire loop extending between the second resistor and the third resistor;

keeping the first wire loop and the second wire loop electrically isolated from each other;

placing the first wire loop and the second wire loop in physical proximity to each other so as to form a protective mesh that envelopes the protected integrated circuit;

providing a detection circuit in operative communication with the trigger circuit and the protected integrated circuit, the detection circuit including ~~includes~~ a first transistor and a second transistor, the first transistor being ~~is~~ operatively connected across the second resistor so that the first transistor is controlled ~~allowed to develop~~ by a bias voltage across the second resistor, the second transistor being ~~is~~ operatively connected across the first transistor and ground so that the second transistor is activated by an output current received from the first transistor, the detection circuit monitoring a flow of current through the trigger circuit, wherein if the flow of current through the trigger circuit is altered because of an open condition in the first wire loop or the second wire loop or a short between the first wire loop and

the second wire loop then the detection circuit outputs a predetermined signal at a ~~and the~~ designated node ~~is~~ located between the power source and the second transistor.

15. (Currently Amended) The method of claim 14, wherein:

the detection circuit further includes a fourth ~~forth~~ resistor connected between the power source and the second transistor;

the first transistor is a PNP type having an emitter node, a base node and a collector node, the first transistor emitter node is connected between the first resistor and the second resistor, the first transistor base node is connected between the second resistor and the third resistor;

the second transistor is a NPN type having an emitter node, a base node and a collector node, the second transistor base node is connected to the first transistor collector node, the second transistor emitter node is connected to ground, the second transistor collector node is connected to the fourth ~~forth~~ resistor; and

the designated node is between the fourth ~~forth~~ resistor and the second transistor collector node.

16. (Currently Amended) The method of claim 15, wherein~~:~~ the predetermined signal is a high voltage condition substantially equal to the power source.

17. (Currently Amended) A method of detecting an attempt to tamper with a protected integrated circuit, the method comprising ~~the step(s) of~~:

providing a power source;

providing a trigger circuit including a plurality of resistors and a plurality of wire loops, the plurality of resistors including a first resistor, a second resistor and a third resistor, all of which being wired together in series and operatively connected to the power source, the plurality of wire loops including a first wire loop extending between

the first resistor and the second resistor and a second wire loop extending between the second resistor and the third resistor;

keeping the first wire loop and the second wire loop electrically isolated from each other;

placing the first wire loop and the second wire loop in physical proximity to each other so as to form a protective mesh that envelopes the protected integrated circuit;

providing a ground layer in physical proximity to the first wire loop or the second wire loop;

providing a detection circuit in operative communication with the trigger circuit and the protected integrated circuit, the detection circuit including a first transistor and a second transistor, the first transistor being operatively connected across the second resistor so that the first transistor is controlled by a bias voltage across the second resistor, the second transistor being operatively connected across the first transistor and ground so that the second transistor is activated by an output current received from the first transistor, the detection circuit monitoring a flow of current through the trigger circuit; and

if the flow of current through the trigger circuit is altered because of an open condition in the first wire loop or the second wire loop or a short between the first wire loop and the second wire loop or a short between the first wire loop or the second wire loop and the ground layer, then outputting a predetermined signal at a designated node of the detection circuit located between the power source and the second transistor.

18. Cancelled.

19. Cancelled.

20. (Currently Amended) The method of claim 17 ~~19~~, wherein:

the detection circuit further includes a fourth ~~forth~~ resistor connected between the power source and the second transistor;

the first transistor is a PNP type having an emitter node, a base node and a collector node, the first transistor emitter node is connected between the first resistor and the second resistor, the first transistor base node is connected between the second resistor and the third resistor;

the second transistor is a NPN type having an emitter node, a base node and a collector node, the second transistor base node is connected to the first transistor collector node, the second transistor emitter node is connected to ground, the second transistor collector node is connected to the fourth ~~forth~~ resistor; and

the designated node is between the fourth ~~forth~~ resistor and the second transistor collector node.

21. (Currently Amended) The method of claim 20, wherein~~:~~ the predetermined signal is a high voltage condition substantially equal to the power source.

22. (Currently Amended) A ~~The~~ method of ~~claim 17, wherein:~~ detecting an attempt to tamper with a protected integrated circuit, the method comprising:

providing a power source;

providing a trigger circuit including a plurality of resistors and a plurality of wire loops, the plurality of resistors including a first resistor, a second resistor and a third resistor, all of which being wired together in series and operatively connected to the power source, the plurality of wire loops including a first wire loop extending between the first resistor and the second resistor and a second wire loop extending between the second resistor and the third resistor;

keeping the first wire loop and the second wire loop electrically isolated from each other;

placing the first wire loop and the second wire loop in physical proximity to each other so as to form a protective mesh that envelopes the protected integrated circuit;

providing a detection circuit in operative communication with the trigger circuit and the protected integrated circuit, the detection circuit including ~~includes~~ a first transistor and a second transistor, the first transistor being ~~is~~ operatively connected across the second resistor so that the first transistor is controlled by ~~allowed to develop~~ a bias voltage across the second resistor, the second transistor being ~~is~~ operatively connected across the first transistor and ground so that the second transistor is activated by an output current received from the first transistor, the detection circuit monitoring a flow of current through the trigger circuit; and

if the flow of current through the trigger circuit is altered because of an open condition in the first wire loop or the second wire loop or a short between the first wire loop and the second wire loop, then outputting a predetermined signal at a ~~and the~~ designated node ~~is~~ located between the power source and the second transistor.

23. (Currently Amended) The method of claim 22, wherein:

the detection circuit further includes a fourth ~~forth~~ resistor connected between the power source and the second transistor;

the first transistor is a PNP type having an emitter node, a base node and a collector node, the first transistor emitter node is connected between the first resistor and the second resistor, the first transistor base node is connected between the second resistor and the third resistor;

the second transistor is a NPN type having an emitter node, a base node and a collector node, the second transistor base node is connected to the first transistor collector node, the second transistor emitter node is connected to ground, the second transistor collector node is connected to the fourth ~~forth~~ resistor; and

the designated node is between the fourth ~~forth~~ resistor and the second transistor collector node.

24. (Currently Amended) The method of claim 23, wherein the predetermined signal is a high voltage condition substantially equal to the power source.

25. (New) An integrated circuit assembly comprising:

an integrated circuit;

a protective barrier enveloping the integrated circuit, the protective barrier including a first wire loop and a second wire loop electrically isolated from each other, a first end of the first wire loop being coupled to a first end of a first resistor, a second end of the first wire loop being coupled to a first end of a second resistor, a first end of the second wire loop being coupled to a second end of the second resistor, and a second end of the second wire loop being coupled to a first end of a third resistor;

a power source coupled to a first end of the first resistor;

a detection circuit including a first transistor having a first, second and third node, the first node being coupled to the first end of the second resistor, the second node being coupled to the second end of the second resistor, the detection circuit further including a second transistor having a first, second and third node, the first node of the second transistor being coupled to ground, the second node of the second transistor being coupled to the third node of the first transistor, and the third node of the second transistor being coupled to the power source and to an output of the detection circuit, the output of the detection circuit being input to the integrated circuit,

wherein the detection circuit monitors a flow of current through the first and second wire loops, and if the flow of current through the first and second wire loops is altered, the output of the detection circuit changes from a first signal to a second signal.

26. (New) The integrated circuit assembly of claim 25, wherein the protective barrier further comprises:

a ground layer in physical proximity to the first wire loop or the second wire loop,

wherein a short between the first wire loop or second wire loop and the ground layer will cause the flow of current through the first and second wire loops to be altered.